CLAIMS

1. A security component for use with an Internet browser application which displays Internet resources in response to resource locators specifying the Internet resources, the security component being adapted to operate alongside the Internet browser application at a user terminal; the security component comprising:

means for storing a plurality of resource locator patterns, each resource locator pattern matching one or more resource locators relating to Internet resources known or believed to be associated with security risks;

means for receiving a resource locator from the browser application;

means for comparing the received resource locator to the stored resource locator patterns;

and means for providing a security alert if the received resource locator matches one of the stored resource locator patterns.

2. A component according to Claim 1, wherein the resource locators are character strings and the resource locator patterns are character patterns.

3. A component according to Claim 2, wherein the comparing means comprises means for testing the resource locator for the presence of one or more characters specified by a character pattern.

4. A component according to any of the preceding claims, adapted to process a pattern comprising one or more wildcards or placeholders.

5. A component according to any of the preceding claims, further comprising means for receiving pattern update information; and means for updating the resource locator patterns stored by the storing means in response to the update information.

6. A component according to any of the preceding claims, further comprising means for transmitting a representation of the resource locator to

a security information server, and means for receiving security information relating to the resource locator from the security information server.

7. A component according to Claim 6, wherein the representation comprises a check sum or hash code of at least part of the resource locator, further comprising means for generating the check sum or hash code.

8. A component according to Claim 6 or 7, wherein the security information comprises a risk rating specifying an estimate of security risk associated with the resource locator.

9. A component according to any of Claims 6 to 8, wherein the security information comprises an indicator indicating whether the resource locator is associated with a trusted Internet location.

10. A component according to any of Claims 6 to 9, wherein the security information comprises IP registration information relating to an IP address with which the resource locator is associated.

11. A component according to any of Claims 6 to 10, further comprising means for displaying the security information.

12. A component according to any of the preceding claims, wherein the alerting means is adapted to prevent the Internet browser application from displaying the Internet resource specified by the resource locator.

13. A component according to any of the preceding claims, further comprising means for receiving an indication of a suspected security risk from a user of the Internet browser application relating to an Internet resource viewed by the user, and means for transmitting the indication to a security information server.

14. A security component for use with an Internet browser application which displays Internet resources in response to resource locators

specifying the Internet resources; the security component comprising means for receiving a resource locator from the browser application; means for transmitting a representation of the resource locator to a remote server; means for receiving IP registration information relating to the resource locator from the remote server; and means for displaying the IP registration information.

15. A security component according to any of the preceding claims, comprising a user interface for user interaction with the security component, the user interface being adapted to be integrated into the user interface of the Internet browser application.

16. A security component according to Claim 15, wherein the user interface comprises a display area for displaying security information relating to the resource locator.

17. A plug-in for an Internet browser application comprising a component as claimed in any of Claims 1 to 16.

18. A toolbar for an Internet browser application comprising a component as claimed in any of Claims 1 to 16.

19. A security information server comprising:

a database of security information relating to Internet locations;

means for receiving a security information request comprising a representation of a resource locator from a user terminal;

means for retrieving security information relating to the resource locator from the database; and

means for transmitting the security information to the user terminal.

20. A security information server according to Claim 19, further comprising:

means for receiving security information relating to a specified resource locator from a user terminal; and means for updating the database in dependence on the security information received.

21. A security information server according to Claim 19 or 20, wherein the database is adapted to store a plurality of resource locator patterns, each resource locator pattern matching one or more resource locators relating to Internet resources known or believed to be associated with security risks.

22. A security information server according to Claim 21, further comprising means for receiving an indication of a suspected security risk relating to a specified resource locator from a user terminal; and means for adding a resource locator pattern matching the specified resource locator to the stored resource locator patterns.

23. A security information server according to Claim 21 or 22, further comprising means for receiving pattern version information from a user terminal specifying the version of a local copy of the resource locator patterns held at the user terminal, and means for transmitting pattern update information to the user terminal in dependence on the version information to update the local copy of the resource locator patterns.

24. A security information server according to any of Claims 19 to 23, further comprising means for calculating a risk rating specifying an estimate of security risk associated with an Internet resource or location referred to by the resource locator, and means for transmitting the calculated risk rating to the user terminal.

25. A security information server according to any of Claims 19 to 24, wherein the database is adapted to store information relating to suspected security vulnerabilities associated with an Internet location.

26. A security information server according to Claim 25, further comprising means for assessing whether potential security vulnerabilities are associated with an Internet location.

27. A security information server according to Claim 26, wherein the assessing means is adapted to identify potential security vulnerabilities in dependence on one or more of: the operating system of a web server associated with the location, the version of that operating system, the web server software used by the web server, and the version of that web server software.

28. A security information server according to any of claims 19 to 27, wherein the database is adapted to store registration information relating to a plurality of IP addresses, and wherein the retrieving means is adapted to retrieve registration information relating to an IP address associated with the received resource locator representation.

29. A security information server according to Claim 28, wherein the registration information comprises information relating to the organisation or person to whom the IP address is registered.

30. A security information server according to any of Claims 19 to 29, wherein the database is adapted to store information relating to trusted Internet locations, the security information server further comprising means for determining whether the received resource locator representation relates to a trusted Internet location, the transmitted security information comprising an indicator indicating whether the received resource locator representation relates to a trusted Internet location.

31. A security information server according to Claim 30, wherein the information comprises a list of trusted domain names.

32. A security information server according to Claim 30 or 31, wherein the information comprises a list of trusted IP addresses or IP address ranges.

33. A security information system comprising a security information server as claimed in any of Claims 19 to 32 and a plurality of user terminals each comprising a security component as claimed in any of Claims 1 to 16.

34. A method of providing security information to a user of an Internet browser application which displays Internet resources in response to resource locators specifying the Internet resources, the browser application residing at a user terminal, the method comprising:

storing, at the user terminal, a plurality of resource locator patterns, each resource locator pattern matching one or more resource locators relating to Internet resources known or believed to be associated with security risks;

receiving a resource locator from the browser application;

comparing the resource locator to the stored resource locator patterns;

and providing a security alert if the resource locator matches one of the stored resource locator patterns.

35. A method according to Claim 34, wherein the resource locator is a character string, and the resource locator patterns are character patterns.

36. A method according to Claim 35, wherein the comparing step comprises testing the resource locator representation for the presence of one or more characters specified by a character pattern.

37. A method according to any of Claims 34 to 36, further comprising receiving, at the user terminal, pattern update information; and updating the plurality of stored character patterns in response to the update information.

38. A method according to any of Claims 34 to 37, further comprising:

maintaining, at a security information server, a database of security information relating to Internet locations;

retrieving security information relating to the received resource locator from the database; and

displaying the security information at the user terminal.

39. A method according to Claim 38, further comprising: storing, at the security information server, a plurality of resource locator patterns, each resource locator pattern matching one or more resource locators relating to Internet resources known or believed to be associated with security risks, and transmitting the resource locator patterns to the user terminal.

40. A method according to Claim 39, further comprising receiving an indication of a suspected security risk relating to a specified resource locator from a user terminal; and adding a resource locator pattern matching the specified resource locator to the plurality of resource locator patterns stored at the security information server.

41. A method according to Claim 39 or 40, further comprising:

transmitting pattern version information from the user terminal to the security information server identifying the version of the local copy of the resource locator patterns held at the user terminal, and

transmitting pattern update information from the security information server to the user terminal in dependence on the version information to update the local copy of the resource locator patterns.

42. A method according to any of Claims 38 to 41, comprising calculating, based on information stored in the security information database, a risk rating specifying an estimate of security risk associated with an Internet resource or location represented by the received resource locator, and displaying the calculated risk rating at the user terminal.

43. A method according to any of Claims 38 to 42, further comprising storing information relating to suspected security vulnerabilities associated with an Internet location in the database.

44. A method according to Claim 43, further comprising assessing an Internet location to determine whether potential security vulnerabilities are associated with the location, and storing the outcome of the assessment in the database.

45. A method according to Claim 44, wherein the assessing step comprises identifying potential security vulnerabilities in dependence on one or more of: the operating system of a web server associated with the location, the version of that operating system, the web server software used by the web server, and the version of that web server software.

46. A method according to any of Claims 38 to 45, further comprising storing registration information relating to a plurality of IP addresses in the database, and wherein the retrieving step comprises retrieving registration information relating to an IP address associated with the received resource locator.

47. A method according to any of Claims 38 to 46, further comprising storing information relating to trusted Internet locations in the database, and wherein the retrieving step comprises determining whether the received resource locator relates to a trusted Internet location.

48. A method according to Claim 47, wherein the information comprises a list of trusted domain names.

49. A method according to Claim 47 or 48, wherein the information comprises a list of trusted IP addresses or IP address ranges.

50. A method according to any of Claims 34 to 49, wherein the alerting step comprises preventing the Internet browser application from displaying the Internet resource specified by the resource locator.

51. A method of providing security information to a user accessing via the Internet accounts for holding or managing money or other tokens of value, comprising:

storing domain names and/or IP address information relating to trusted Internet sites providing access to such accounts;

receiving a resource locator specifying an Internet resource requested by the user;

determining whether the resource locator relates to a trusted Internet site by comparing a domain name or IP address associated with the resource locator to the stored domain names and/or IP address information; and

outputting a corresponding indication to the user if it is determined that the resource locator does relate to a trusted Internet site.

52. A component, plug-in or toolbar for an Internet browser application adapted to carry out a method as claimed in any of Claims 34 to 51.

53. A security information server adapted to carry out a method as claimed in any of Claims 34 to 51.

54. A computer program or computer program product comprising a security component as claimed in any of Claims 1 to 16.

55. A computer program or computer program product comprising software code adapted, when executed on a data processing apparatus, to perform a method as claimed in any of Claims 34 to 51.

56. A component, plug-in or toolbar for use with an Internet browser application substantially as described herein with reference to and as illustrated in Figures 1 to 5 of the accompanying drawings.

57. A security information server substantially as described herein with reference to and as illustrated in Figures 1, 2 and 6 of the accompanying drawings.

58. A security system substantially as described herein with reference to and as illustrated in Figures 1 to 6 of the accompanying drawings.

59. A method of providing security information substantially as described herein with reference to and as illustrated in Figures 1 to 6 of the accompanying drawings.